Remarks:

Applicant appreciatively acknowledges the Examiner's confirmation of receipt of applicant's claim for priority and certified priority document under 35 U.S.C. § 119(a)-(d).

Reconsideration of the present application is respectfully requested.

Claims 2 - 7 and 11 - 18 are now pending. Claims 1 and 8 - 10 have been cancelled. New claims 11 - 18 were added to the application.

In paragraph 2 on page 2 of the above-identified Office action, the oath or declaration was objected to as defective because the title of the invention identified in the declaration did not match the title identified in the specification. Applicant will submit a substitute declaration identifying the present application, prior to payment of the issue fee in the present case.

In paragraph 3 of the above-identified Office action, the specification has been objected to due to two informalities. The specification has been amended to address the issues raised in the Office Action.

In paragraphs 4 and 5 of the Office Action, claims 1 - 3 and 7 were rejected under 35 U.S.C. § 112, second paragraph.

It is believed that the rejections of claim 1 in paragraph 5a-b of the Office Action are moot in view of the cancellation of that claim.

Claims 2, 3 and 7 have been amended to address the issues cited in the rejection of those claims in paragraphs 5c, 5d and 5e of the Office Action.

It is accordingly believed that the specification and the claims meet the requirements of 35 U.S.C. § 112.

In paragraphs 6 - 7 of the Office action, previously pending claims 1 - 10 were rejected as allegedly being anticipated under 35 U.S.C. § 102(b) by Jablon, "Strong Password-Only Authenticated Key Exchange," *ACM Computer Communications Review*, October 1996 ("**JABLON**"). Independent claims 1 and 10 and dependent claims 8 and 9 have been canceled from the present application. Remaining dependent claims 2 - 7 have been amended to ultimately depend from new claim 11. As will be discussed herein, Applicant believes that all claims currently pending are patentable over the **JABLON** reference.

Before discussing the prior art in detail, it is believed that a brief review of the invention as claimed, would be helpful. Presently pending independent claim 11 recites an authenticating method, comprising the steps of,

> "a) performing a first operation by a first entity on a prescribed known value and on a value only known to the first entity to obtain an uncoded result of the first operation;
>
> b) encoding the result of the first operation with a first key known to the first entity and to a second entity to obtain an encoded result of the first operation;
>
> c) transferring a message from the first entity to the second entity, wherein the message comprises the encoded result of the first operation as well as the uncoded result of the first operation; and
>
> d) decoding the encoded result of the first operation by the second entity with the first key and authenticating the first entity only using the message."

Among other limitations, independent claim 11 requires the transfer from a first entity to a second entity, **both** the **encoded result** of a particularly claimed first operation, as well as, the **uncoded result** of the claimed first operation. Similarly, independent claim 18 recites an authenticating arrangement comprising, among other limitations, a first entity arranged to transfer to a second entity **both** the **encoded result** of a particularly claimed first operation and the **uncoded result** of the claimed first operation.

Systems in the art have transmitted an encrypted message and a plain text message from a first entity to a second entity. In these systems the messages are interpreted at the second entity by either: 1) decrypting the encrypted part of the message to compare with the plain text for identity; or 2) encrypting the plain text to compare with the encrypted message for identity. These systems did not:

> "[perform] a first operation by a first entity on a prescribed known value and on a value only known to the first entity to obtain an uncoded result of the first operation;"

And

> "[transfer] a message from the first entity to the second entity, wherein the message comprises the encoded result of the first operation as well as the uncoded result of the first operation;"

As done by Applicant's claimed invention. Claim 18 recites similar limitations.

Further, the **JABLON** reference fails to teach or suggest Applicant's claimed invention. **JABLON** discloses a simple password exponential key exchange method. In the Office Action, in rejecting the formerly presented claim 1, Applicant was directed to section 3.2 of **JABLON** which described the Diffie-Hellman Encrypted Key Exchange ("**DH-EKE**"). In the **DH-EKE** system described in **JABLON**, the system uses a DH exchange to establish a shared key K. Relative to an example given in **JABLON**, Alice and Bob agree on a common base and a module. Alice generates a random number (R_A) and calculates a modular exponentiation (Q_A) using the base and module and with the random number as the exponent. Alice encodes this expression with a secret password (S) shared by Alice and Bob. Alice transmits the encoded result ($E_s(Q_A)$)of the modular exponentiation to Bob. Bob decodes the message received from Alice, produces an extra random number, calculates a modular exponentiation using the extra random number (R_B) as the exponent, encodes the result of this modular exponentiation with the password (S) and transfers the encoded result ($E_s(Q_B)$) of the modular exponentiation to Alice. Alice decodes the received encoded message and, like Bob, produces a secret key (K) for the future communication, wherein the secret key (K) is calculated from a modular exponentiation in which the product of the random numbers of Bob and Alice corresponds to the exponent and a subsequently performed hashing function (h).

An authentication will only take place when Bob and Alice are able to exchange messages with the newly-produced key (K) and communicate to each other in a useful way. If no useful communication is possible, the keys of Bob and Alice do not match, which indicates that either Bob or Alice have not been authentic. As such, **JABLON** does not teach or suggest sending a "**message**" including **both** an **encoded** and an **uncoded** result of an operation, as required by Applicant's claims. Instead, **JABLON** either discloses transferring only the uncoded result of an operation and not the encoded result, or transferring only the encoded result of an operation and not the uncoded result. Alternatively, **JABLON** also discloses transferring a message from Alice to Bob that is encoded, while the message from Bob to Alice is uncoded.

Further, As can be seen from the claims, Applicant's invention authenticates the first entity to the second entity with the transmission of only the claimed **message**. For example, step d of Applicant's independent claim 11 recites, among other limitations,

> "decoding the encoded result of the first operation by the second entity with the first key and authenticating the first entity **only using the message**." [emphasis added]

JABLON does not authenticate using only a single message. Rather, studying the operation of the systems described in **JABLON**, if Alice does not know the mutual password (S), but uses another password, Bob still will receive a message from Alice, albeit one encoded with the wrong password. Bob will still decode the message with the correct password and, of course, will obtain some result. Bob then encodes his part, i.e., the result of his modular exponentiation, with his selected random number and with the correct password and transmits that encoded message to Alice. Alice decodes this message with the wrong password and, of course, will still obtain some result. Both Bob and Alice now calculate a "symmetrical" key by a multiplication of the respective self-produced result of the modular exponentiation by the decoded result of the modular multiplication received from the other, which will, of course, be incorrect due to the use of different passwords.

In the example of **JABLON**, it can be seen that up to this point Bob does not know that Alice is not authentic. It is only when Bob and Alice try to communicate with each other that they realize that no sensible communication is possible, since they used different keys in a symmetrical cryptography operation. It is only at this late stage that Bob will realize that Alice is not authentic. One disadvantage to the late stage realization of Alice's failure to be authentic is that Bob, nevertheless, was required to send an encoded message to Alice, even though she is not authentic. Under the system of section 3.2 of **JABLON,** there was no way for Bob to realize this in time. Non-authentic Alice thus succeeds in drawing out a message from Bob which includes both his random exponent and the password, in some form. This results in a safety breach of the system caused by the failure to authenticate Alice at an early stage, before Bob was required to transmit.

In contrast, according to Applicant's claimed invention, due to the transfer of the result of the first operation in both plain text and encoded with the password, an authentication is only obtained using a single **message** (see step 'd' of claim 1). Thus, Applicant's authentication occurs at a very early stage. A single transmitted **message** is completely sufficient. Thus, Applicant's claimed invention provides a safer authenticating method and system than that described in **JABLON**. In Applicant's claimed method and system, Bob would succeed in establishing Alice's inauthenticity when receiving and evaluating the first message from Alice. Bob can take informed measures, such as, cutting off communication with Alice immediately, so as to not transfer secret information, generated using his password or secret exponent to a potential attacker. Applicant's claim 18 contains similar features.

It is accordingly believed that **JABLON** fails to teach or suggest the features of independent claims 11 or 18. Claims 11 and 18 are, therefore, believed to be patentable over the art. The dependent claims are believed to be patentable as well because they all are ultimately dependent on claim 11.

In view of the foregoing, reconsideration and allowance of claims 2 - 7 and 11 - 18 are solicited.

In the event the Examiner should still find any of the claims to be unpatentable, counsel would appreciate receiving a telephone call so that, if possible, patentable language can be worked out.

If an extension of time for this paper is required, petition for extension is herewith made.

Please charge any fees that might be due with respect to Sections 1.16 and 1.17 to the Deposit Account of Lerner and Greenberg, P.A., No. 12-1099.

Respectfully submitted,

For **Applicant**

Kerry P. Sisselman
Reg. No. 37,237

KPS:cgm

November 9, 2004

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101